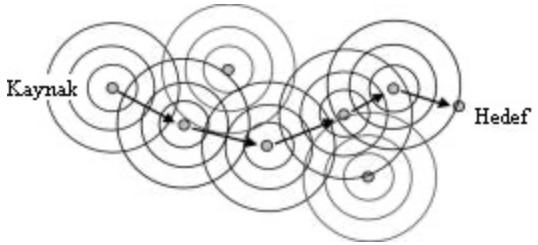
Tasarsız (Ad-Hoc) Ağlarda Güvenlik

Akış

- Giriş
- Güvenlik Sorunlarının Nedenleri
- Güvenlik Hedefleri
- Ağ Katmanlarında Güvenlik Önlemleri
- Sonuç

Tasarsız ağ karakteristikleri

- Sabit bir altyapı ve merkezi sunucu yok: benzer bileşenler
- Kendiliğinden yapılanma
- Belirli bir amaç: geçici ağ hizmeti
- Rastgele ve hemen kurulum
- Düğümlerin hareketliliği
  - dinamik topoloji değişikliği
- Düğüm fonksiyonu:
  - topoloji değişimini farketmek
  - yönlendirme
- Sınırlı kaynaklar, kısa menzil



Tasarsız ağ kategorileri-1

- NIST (National Institute of Technology)

1. Gezgin tasarsız ağlar
   (Mobile ad hoc Networks, MANETs)
2. Duyarga ağları
   (Wireless Ad Hoc Sensor Networks)

Tasarsız ağ kategorileri-2

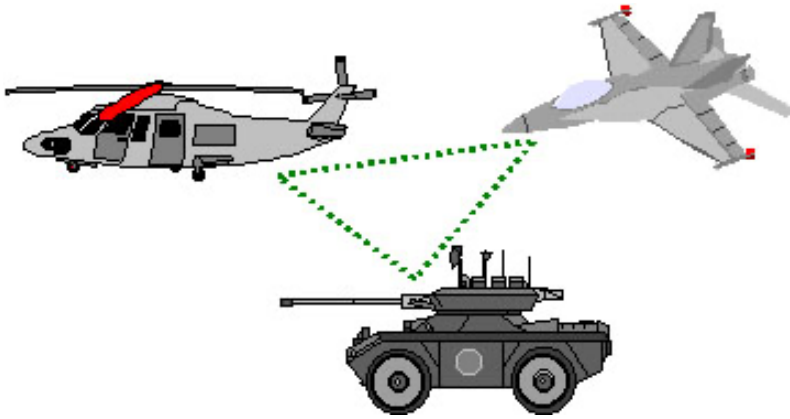
- MANET: sivil uygulamalar

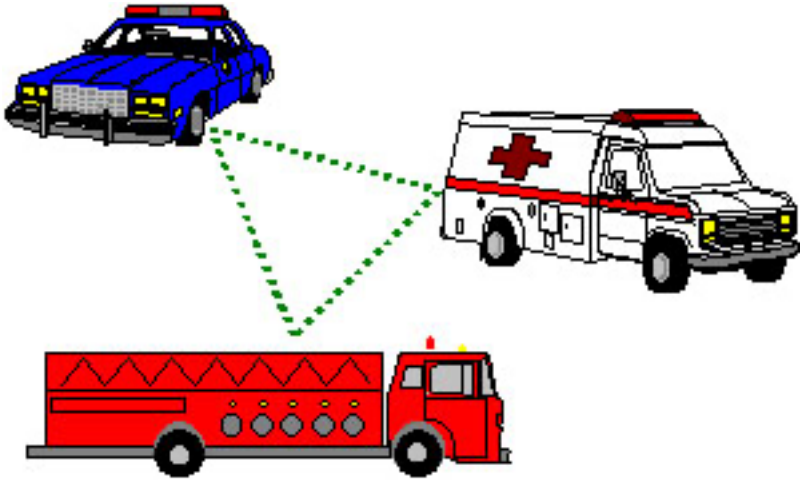
  laptop, PDA, cep telefonu

- Duyarga ağları: daha çok askeri amaçlı
  - düğüm sayısı, kısıtlar daha fazla
  - güvenlik çok daha önemli
  - iletişimin sezilmemesi; düşük güç

Tasarsız ağ uygulamaları

Askeri operasyonlarda





İlk yardım çalışmalarında

Tasarsız ağ uygulamaları

- Toplantı veya konferanslarda
- Ticari amaçlı:
  - Sergi
  - Satış
- Yasal zorunluluk

Güvenlik Hedefleri

- Ulaşılabilme
- Asıllama
- Bütünlük
- Güvenirlik
- İnkar edememe

Ulaşılabilme

- Ağ hizmetlerinin DoS saldırılarına rağmen varlığını koruması
  - Ağa mesaj yığma
    frekans sekme, spektrum yayma / otorite
  - Güç tüketme:sleep deprivation torture
    uyku modu

Asıllama

- Haberleşilen düğümün iddia ettiği düğüm olup olmadığının sınanması
  - Merkezi bir sunucuya güvenilemez

Bütünlük

- Mesajın bütünlüğünün bozulmayacağı garantisi
  - bozucu etkenler
  - kötü niyetli saldırılar

Güvenilirlik

- Bilginin yetkisi olmayan kullanıcılara açılmaması
  - asıllama ile

İnkar edememe

- Mesajı gönderenin göndermediğini iddia etmesinin önlenmesi
  - hatalı mesaj

Ağ Katmanlarında Güvenlik

- Kötü niyetli düğümlerin davranışlarının önüne geçebilmek için katmanlı bir güvenlik mekanizması

Katman	Güvenlik Konuları
Uygulama	Zararlı kodları, sızmaları belirleme
Ulaşım	Asıllama ve veri şifreleme ile uçtan uca iletişim güvenliğinin sağlanması
Ağ	Yol atama protokollerine saldırıları önleme
Veri bağı	MAC protokolünün korunması ve bağ katmanı güvenlik desteği
Fiziksel	İşaretleri hizmetlere saldırıdan(DoS) korumak

Fiziksel katmanda güvenlik

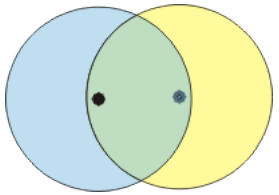
- Frekans sekmeli güvenlik önlemi
  - dinlenme
  - yol kesme
  - değiştirme
  - düşürme

Veri bağı katmanında güvenlik

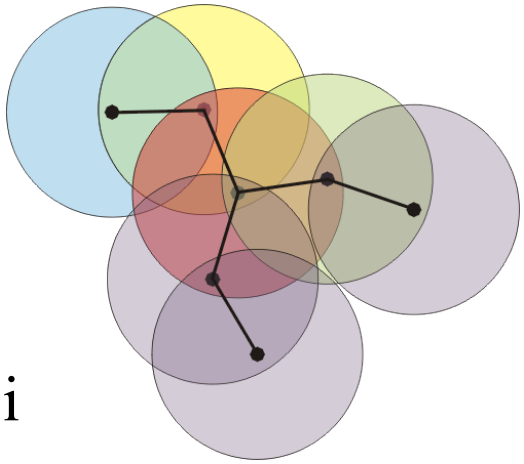
- Kötü niyetli düğüm
  - NAV'ın boyunu değiştirebilir
  - komşu düğümlerin boş(idle) kalacağı zaman dilimi için büyük sayılar atayabilir
  - çerçeveler arası boşlukları(SIFS,DIFS) azaltabilir
  - küçük geri çekilme değerleri seçebilir *

Ağ katmanında güvenlik

- Tasarsız gezgin ağlarda çok sekmeli bağlantı 2 aşamada sağlanır:



1. Bağ katmanı protokolleri üzerinden tek sekmeli bağlantının sağlanması



2. Kurulan bağlantının ağ katmanında *yol atama* ve veri iletimi protokolleri ile çok sayıda sekmeye genişletilmesi

Yol atama teknikleri

- Yapılarına göre:

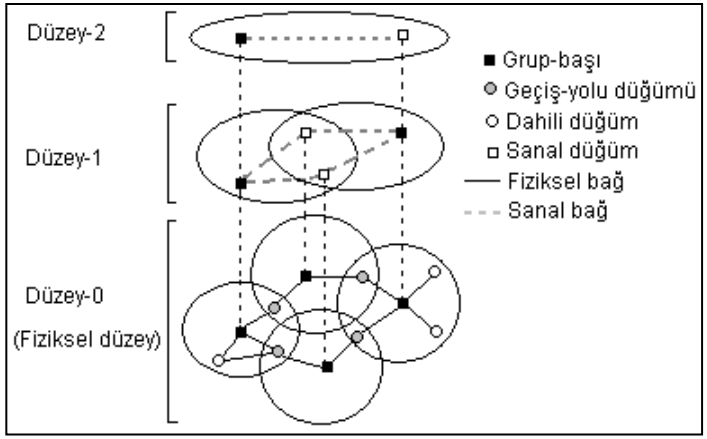
  1. Yatay yol atama (flat routed)

  Her düğüm ağdaki diğer bütün düğümlere giden yol bilgilerinin bulunduğu bir yol atama tablosu tutar.

  - işlem yükü

  2. Hiyerarşik yol atama

  - öbekler
  - en iyi yol bulunamaz



Yol atama protokolleri

- 3 sınıfta incelenebilir:

  1- Tabloya dayalı yol atama (Proactive): DSDV
  - tüm varışlara sürekli yol
  - genelde en kısa yol
  - yol atamada gecikme az

  2- İstekle tetiklenen yol atama (Reactive): DSR, AODV
  - sadece iletişim istendiğinde
  - herhangi bir yol
  - kaynak kullanımı+

  3- Hibrid yol atama

Yol atama protokollerine saldırı

- 3 sınıfta toplanabilir:
  1. Değişiklik yaparak saldıranlar (modification)
  2. Taklit ederek saldıranlar (impersonation)
  3. Asılsız veri ile saldıranlar (fabrication)

- IETF: AODV ve DSR

Değişiklik yaparak saldıranlar

- Denetim mesajlarını değiştirerek veya yönlendirme bilgisindeki değerleri çarpıtarak hizmeti yadsıma (DoS) ve ağ trafiğini yeniden yönlendirme

1. Değiştirilmiş yol sıra numaraları ile yeniden yönlendirme
2. Değiştirilmiş sekme sayısı ile yeniden yönlendirme
3. Değiştirilmiş kaynak yolu ile DoS
4. Tünel saldırısı (solucan deliği)

1.Değiştirilmiş yol sıra numaraları ile yeniden yönlendirme

- AODV, DSDV
- Varış noktalarına giden yollara monoton artan sıra numaraları
- Daha yüksek sıra numaralı yol tercihi

AODV'de herhangi bir düğüm, gerçek değerinden daha büyük bir varış sıra numarasına sahip yolun varlığını ilan ederek trafiği kendine çekebilir.

2.Değiştirilmiş sekme sayısı ile yeniden yönlendirme

- AODV'de sekme sayısı alanını ile en kısa yolum tayini
- Kötü niyetli düğümler RREQ'da
  - sekme sayısı alanını sıfırlayarak yeni oluşturulacak yolda yer alma şanslarını arttırırlar.
  - sekme sayısı alanını sonsuza götürerek oluşturulacak yolda bulunmamayı sağlayabilirler.

3.Değiştirilmiş kaynak yolu ile DoS

- DSR’de kaynak yol mekanizması
- Kullanılan yollar veri paketinde açıkça belirtilir.
- Bu yollarda herhangi bir bütünlük denetimi söz konusu değildir.
- Basit bir hizmeti yadsıma saldırısı (DoS) paket başlıklarındaki kaynak yollar değiştirilerek gerçekleştirilebilir.

4. Tünel saldırısı

- 2 ya da daha cok düğümün varolan veri yolları üzerinde mesaj değiş tokuş etmek üzere birlikte çalışması durumunda
- Mevcut çok sekmeli yollar üzerinde tünel kurmak yerine aralarındaki uzun menzilli yönlü telsiz ya da telli bağlantıların kullanımı

Taklit ederek saldıranlar

- Düğüm kendisinden çıkan paketlerde IP ya da MAC adresinde değişiklik yapıp kimliğini bilerek yanlış gösterirse

Asılsız veri ile saldıranlar

- Sahte yol atama mesajları
- Yalancı hata mesajı: “komşu bağlantısı kurulamıyor”
- Tespiti çok kolay değil

1. AODV ve DSR’de yol hatalarını çarpıtmak

   Sürekli gönderilen ve yol üzerindeki bağlantıyı kopmuş gibi gösteren yol hata mesajları (DoS)

2. DSR’de yol kayıtlarını zehirlemek

   DSR’de kulak misafiri düğüm paket başlığındaki yol atama bilgisini kendi yol kayıtlarına ekleyebilir. Saldırgan paket başlıklarında geçersiz yol içeren paketleri aktararak yol kayıtlarını zehirleyebilir.

$$F(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$$

Önerilen yol atama protokolleri

- Öneriler
  - SRP
  - ARIADNE
  - ARAN
- Genel Bakış
  - AODV ve DSR üzerine geliştirme ve iyileştirme
  - Bencillik problemini ele almaz
  - Kontrollü ortam

SRP (Secure Routing Protocol)-1

- Varsayım : Kaynak ve hedef arasında simetrik gizli bir anahtar
- İşleyiş : B başlangıç, V varış

  Kaynak : $K_{B,V}$ ile mesaj asıllama kodunu(MAC) üretir

  Ara düğüm: RREQ'i varışa doğru iletirken diğer düğümlerden gelen sorgulama sıklığına göre düğümlere ters orantılı bir öncelik değeri atar.
    - ağı kirleten kötü niyetli düğümler düşük öncelik öncelikli

  Hedef : İstenen alanların hash'ini hesaplar SRP başlığındaki MAC ile karşılaştır.
    - RREQ'in asıllığının ve bütünlüğünün denetimi

  Hedefin gönderdiği RREP ile MAC sınaması

SRP (Secure Routing Protocol)-2

- (+) eşleşmeyen belirteçler ile tekrar saldırılarının önlenmesi
- (+) asıllama ile değişiklik ve asılsız yol atama sınaması
- (-) asılsız veri ile yol kayıtlarının zehirlenmesi:
  ara düğüm cevap jetonu (INRT)
- (-) yol koruma mesajlarının onaylanması mekanizması:
  kötü niyetli düğüm sadece üzerinde olduğu yola zarar verebilir.
- (-) solucan deliği saldırısı

ARIADNE-1

- Varsayım: Kaynak ve hedef arasında paylaşılan gizli bir anahtar
  Her düğüm için güvenilir bir anahtar
- İşleyiş : <ROUTE REQUEST, başlangıç, varış, id, zaman aralığı,
  hash zinciri, düğüm listesi, MAC listesi >

  Kaynak : $MAC_{KB,V}$ (başlangıç, varış, id, zaman aralığı)

  Ara düğüm: <başlangıç, id>
  hash zinciri->H(düğüm adresi, hash zinciri)
  MAC(RREQ) : KAi TESLA anahtarı, i:zaman aralığı

  Hedef : belirtilen anahtarların zaman aralığında geçerliliği ve
  hash zinciri denetimi ->RREQ onayı
  <ROUTE REPLAY, varış, başlangıç, zaman aralığı, düğüm listesi, MAC listesi, hedef MAC, anahtar listesi>

ARIADNE-2

- (+) varış düğümünün başlangıç düğümünü asıllaması
- (+) başlangıç düğümünün gelen RREP mesajında sunulan ve hedefe giden yol üzerindeki tüm ara düğümleri asıllaması
- (+) ara düğümlerin de RREQ ve RREP mesajlarındaki düğüm listesinden bir önceki düğümü silemeyeceğinin garantisi
- (-) bencil düğümleri hesaba katmaz

ARAN-1

- Varsayım: Güvenilir bir sertifika sunucusu (C)
  Her düğümün C tarafından verilen bir sertifikası var
  - IP, açık anahtar, zaman damgası
- İşleyiş : 1.ön ruhsatlandırma süreci
  2.zorunlu bir uçtan uca asıllama aşaması
  3.zorunlu olmayan en kısa güvenli yol aşaması
- Kaynak (A) : [RDP; IPB; sertifikaA; NA; t]K_A
- Ara düğüm(X): [[RDP; IPB; sertifikaA; NA; t] K_A]K_X; sertifikaX
- Ara düğüm(Y): [[RDP; IPB; sertifikaA; NA; t] K_A]K_Y; sertifikaY
- Hedef : [REP; IPA; sertifikaB; NA; t] K_B

SPC; en kısa yol doğrulaması

İç içe imzalanmış ve şifrelenmiş SPC mesajı biçimi ara düğümlerin yol uzunluğunu değiştirerek mesaj bütünlüğünü bozmasını engeller.

ARAN-2

- (+) asıllama ve bütünlük sağlanır
- (+) yolu koruma safhası yol hata paketlerinin de imzalanması ile güvenli hale getirilmiştir.
  - Hata mesajını gönderen düğümün imzası ile inkar edememe ilkesi de sağlanır.
- (+) değiştirme, taklit, uydurma saldırılarına önlem
- (-) asimetrik şifreleme yöntemi CPU ve enerji kullanımı göz önüne alındığında ekonomik değildir

Yol atamada güvenlik gereksinimleri

- Açık ortam

  1. Yol işaretleri aldatılmamalıdır.
  2. Asılsız yol atama mesajlarının ağa girmesi engellenmelidir.
  3. Yol atama mesajları iletimde protokol fonksiyonunun işleyişi dışında değiştirilmemelidir.
  4. Zararlı eylemler dahilinde yol atama döngülerinin oluşturulması engellenmelidir.
  5. Yeniden yönlendirmeye izin verilmemeli, en kısa yollar korunmalıdır.

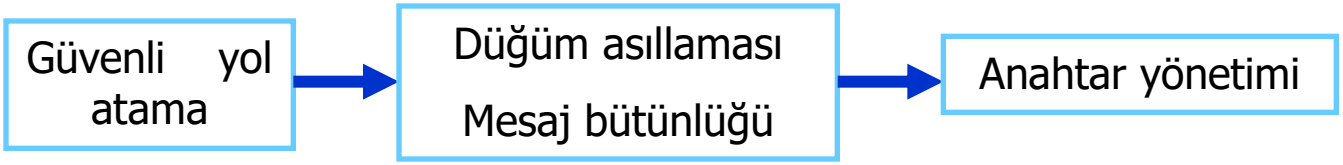
- Kontrollü açık ortam

  +Yetkili olmayan düğümlerin yol bulma ve hesaplamadan men edilmelidir

- Kontrollü düşman ortamı

  +ağ topolojisinin ne düşmana ne de yetkili kabul edilen düğümlere açık bırakılmaması

Ulaşım katmanında güvenlik



- Önerilen güvenli yol atama protokolleri için anahtar yönetimi yaklaşımı iki kategoride toplanabilir:

  1. Simetrik gizli anahtarların düzenlenmesi

  Asıllama ve bütünlüğü sağlamada kullanılacak oturum anahtarını oluşturmak için gizli anahtar

  Örnek: SRP

  2. Açık anahtar tabanlı düzen

  Her düğüm için bir gizli ve açık anahtar çifti

  Örnek: ARAN

PGP'ye dayalı, kendi kendine düzenlenen açık anahtar yönetimi

- Sertifika
  - Kullanıcıların kişisel bilgilerine dayanır
  - Yerel sertifika depolarında saklanır
  - Kullanıcılar tarafından yürütülür/ PGP'den ayrım
- Haberleşme
  - Yerel sertifika depoları birleştirilir
  - Birleşimde uygun sertifikalar aranır
  - Açık anahtarlar onaylanır
- Açık ortam, tasarsız ağ doğasıyla örtüşme
- Yöntemin başarısı: yerel sertifika depolarına ve sertifika graflarının yapısı

Polinom şeklindeki gizli bilgi paylaşımına dayalı asıllama

- Sertifika
  - Bir küme komşu tarafından müşterek üretilir.
  - Grup imzası
- Gizli bilgi paylaşımı
  - Gizli imza anahtarı çok sayıda düğüme dağıtılır.
- Yerleşik güven modeli: Birden fazla düğüm(komşu düğümler) birlikte başka bir düğümün davranışını gözetler, biletini onaylar ya da imha eder.
- Düğümlerin taşıdığı sertifikalar ortak sertifika anahtarı SK ile imzalanmıştır. SK'nın bir şekilde her düğüme iletilmesi gerekir.

  Bu işlemi başlatmak için en az ilk k düğüme bu anahtarın verilmesi gerekir. Bu düğümler işbirliği içinde anahtarı diğer düğümlere yayarlar.
- Kötü niyetli düğümler için suçlama duyurusu

Uygulama Katmanı

- Verilerin şifrelenmesi ya da kullanıcıların asıllanması gibi önlemler tam olarak yeterli değil
  - karşılıklı anlaşan düğümler
- Sistemin ikinci bir savunma mekanizmasına ihtiyacı var
  - Sızma sezme (intrusion detection)

Sızma Sezme Sistemi (IDS)

- Ağdaki şüpheli davranışları algılayıp alarm veren yapı
- Biriktirilmiş denetim bilgileri
- SSS algoritmaları dağıtılmış olmalı
- Denetim bilgilerine erişim zor

Sonuç

- Önerilen çözümler tüm saldırılara birden karşı koyamamaktadır.
- Güvenlik çözümlerinde bazı gerçekçi olmayan varsayımlar yapılmaktadır.
  - anahtar yönetimi için bir yapının var olduğu varsayımı tasarsız ağların altyapısız doğasına aykırıdır
- Tasarsız ağlarda kısıtlı özkaynaklar ile daha da zorlaşan güvenlik konusu çözülmesi gereken ve hala üzerinde çalışılan olan bir sorundur.
- Tasarsız ağlar için geliştirilen teknoloji ilerledikçe daha gerçekçi ve kapsamlı çözümlerin getirilmesi beklenmektedir.